ISPL1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

DAS SEGUROS

Contenido:	Política de Seguridad de la Información
Ámbito de aplicación:	DAS Seguros y Das Lex Assistance
Versión:	2.1
Fecha vigor:	30/08/2019
Estado:	Aprobado
Clasificación:	Pública

Índice

1. Introducción

La seguridad de la información –confidencialidad (no divulgación de información no autorizada), integridad (no realización de cambios sin autorización), y disponibilidad (disponibilidad de la información en concordancia con los requerimientos de los procesos de negocio) es un factor clave de éxito para ERGO y se está volviendo cada vez más importante debido a la digitalización de nuestro negocio. Al mismo tiempo, cada vez es más difícil garantizar la seguridad de la información. Como resultado de esto, se deben abordar riesgos adicionales. Esto se relaciona, entre otras cosas, con el uso de nuevas infraestructuras, como la computación en la nube, sin mencionar el creciente número de ciberataques cada vez más agresivos y sofisticados.

Además, la información sobre clientes, productos y procesos de ERGO no solo se guarda en los ordenadores. Por lo tanto, también los documentos impresos, las notas manuscritas o las conversaciones deben estar adecuadamente protegidos.

Esto no solo se aplica a ERGO sino a toda la economía y a la sociedad, y se refleja en un número cada vez mayor de requisitos reglamentarios y legales. Además, los principios corporativos y las directrices de Munich Re requieren el establecimiento de procesos y procedimientos para la seguridad de la información.

Por esta razón, el Consejo de Administración del Grupo ERGO ha decidido establecer un Sistema de Gestión de Seguridad de la Información (SGSI) en todo el grupo con el fin de alcanzar y mantener los niveles adecuados de seguridad de la información. El SGSI está orientado hacia la norma internacionalmente reconocida ISO / IEC 27001: 2013.

Esta 'Política de seguridad de la información' define los principios de seguridad de la información para todo el Grupo ERGO y por lo tanto toma en cuenta los requisitos legales y regulatorios aplicables. La política sirve como base para la administración de la seguridad de la información y para regulaciones específicas a fin de proteger la confidencialidad, integridad (que incluye además el concepto de autenticidad) y disponibilidad de la información dentro de ERGO contra amenazas internas o externas, ya sean intencionales o no.

Además, la 'Política de Gestión de Continuidad del Negocio de ERGO' establece los requisitos mínimos, los objetivos, las responsabilidades, los procesos y los procedimientos de información para la Gestión de la Continuidad del Negocio (PCN).

Por lo tanto, SGSI y PCN respaldan a ERGO en la protección de la información, así como en la recuperación de negocios de situaciones de emergencia y crisis.

2. Alcance de la Política

La Política de Seguridad de la Información será aplicable a todos los trabajadores de **DAS SEGUROS** y **DAS Lex Assistance (en adelante Grupo DAS)** sean o no empleados indefinidos, temporales o de ETT's, incluyendo cualquier persona ajena a **Grupo DAS** que tenga acceso a la información gestionada o propiedad de la misma. La Política también será aplicable a toda la información en soporte digital y a los sistemas de Información propiedad de o gestionados para **Grupo DAS**.

3. Responsabilidad para la seguridad de la información

El Consejo de Administración del Grupo ERGO encarga al Director de Seguridad de la Información (CISO) que establezca la estrategia de seguridad de la información en coordinación con el CIO Global del Grupo ERGO y defina, dirija, supervise y desarrolle aún más el Sistema de Gestión de Seguridad de la Información (SGSI) de ERGO.

El CISO define y mantiene los requisitos de seguridad de la información para todo el grupo y los desarrolla en forma más concreta para la seguridad de la información, los servicios compartidos de grupo relevantes (continuidad de negocio, compras, gestión de instalaciones, seguridad TI, Recursos Humanos, etc.). El papel del CISO es parte de la función de gestión de riesgos independiente (2da línea de defensa). En esta función, el CISO establece disposiciones para la identificación y control consistentes de los riesgos de seguridad de la información y que la organización del SGSI está estandarizada. El CISO puede escalar, si es necesario, temas relevantes de seguridad de la información directamente al miembro responsable para la seguridad de la información del Consejo de Administración del Grupo ERGO.

La gestión operativa (primera línea de defensa) es responsable de definir, implementar y controlar las medidas de seguridad de la información para el manejo de riesgos y el cumplimiento de los requisitos de seguridad de la información.

Cada empleado, contratista y usuario externo de Grupo DAS (por ejemplo, un socio de ventas) garantiza dentro de su área de responsabilidad que la información del cliente y de la empresa esté protegida de manera apropiada.

4. Principios de la seguridad de la información

4.1 Gobierno basado en riesgo de seguridad de la información

No es posible proporcionar seguridad total para toda la información. Además, no toda la información requiere la misma protección. Grupo DAS, por lo tanto, gestiona la seguridad de la información basado en el riesgo. Esto hace posible que Grupo DAS facilite y use recursos en las áreas donde más urgentemente se requieren. El CISO de Grupo ERGO, por esta razón, define los requisitos unificados para la gestión de los riesgos de seguridad de la información y, por lo tanto, facilita y supervisa las decisiones basadas en el riesgo.

4.2 Cada empleado es conocedor de su responsabilidad individual en la seguridad de la información

Tanto los empleados internos como externos de Grupo DAS se encuentran entre los factores de éxito más importantes para garantizar los niveles de seguridad de la información requeridos. Numerosas medidas de seguridad solo pueden implementarse eficazmente si los empleados internos y externos son suficientemente conscientes de la seguridad de la información y tienen suficientes habilidades en el campo de la seguridad de la información. El CISO, por lo tanto, desarrolla un concepto que sirve como base para definir las medidas de concientización y capacitación centradas en los grupos objetivo que luego son proporcionadas por el Grupo ERGO y las empresas ERGO.

4.3 Cumplimiento de requisitos mínimos unificados de seguridad de la información

El nivel de seguridad de la información que se requiere en todo el Grupo solo puede garantizarse mediante requisitos mínimos unificados y vinculantes y sus características

locales. Por esta razón, hay cuatro niveles de política de seguridad de la información (ISPL en inglés) basados el uno en el otro:

- Esta Política de Seguridad de la Información (ISPL1) describe en el nivel superior los principios y objetivos de la seguridad de la información del Grupo ERGO.
- Los documentos ISPL2 definen los requisitos de seguridad de información para todo el Grupo. Se aplican a todas las empresas ERGO nacionales e internacionales que se especifican en el documento respectivo.
- Los documentos ISPL3 establecen en detalle los requisitos de los documentos ISPL2 en forma de requisitos detallados para cada empresa ERGO o para los servicios compartidos de Grupo ERGO relacionados con la seguridad de la información.
- Los documentos ISPL4 describen las instrucciones específicas para los procesos, los procedimientos y las medidas de seguridad de la información para cumplir con los requisitos de los documentos ISPL2 e ISPL3.

El CISO crea y mantiene la Política de Seguridad de la Información de ERGO, los documentos ISPL2 y los documentos ISPL3 para todos los servicios compartidos por el Grupo. Las empresas ERGO desarrollan los requisitos de los documentos ISPL2 en documentos ISPL3 específicos locales para todos los servicios relevantes de seguridad de la información que no reciben como servicios compartidos de grupo. Los documentos ISPL4 son creados y mantenidos por las unidades funcionales responsables respectivamente.

Si los requisitos definidos por el CISO no se pueden cumplir por razones legales, reglamentarias o funcionales, la coordinación con la unidad de seguridad de la información del Grupo ERGO es obligatoria.

4.4 Cooperación orientada a la seguridad con partes externas

La cooperación con proveedores y socios de servicios externos no debe reducir el nivel de seguridad de la información de Grupo DAS. Por esta razón, los proveedores y los socios de servicios externos solo pueden tener acceso a la información de Grupo DAS y los recursos de TI una vez que Grupo DAS ha evaluado y clasificado los niveles de seguridad de la información de los proveedores y socios de servicios externos según corresponda. Además, Grupo DAS solo otorga acceso a información y recursos de TI que son necesarios para la cooperación (principio de necesidad de conocer). El CISO, por lo tanto, define los requisitos unificados para la cooperación orientada a la seguridad con partes externas.

4.5 Desempeñar una parte activa en mantener el nivel de protección

Los niveles de seguridad de la información requeridos deben verificarse, monitorearse y evaluarse de manera independiente para poder mantenerlos y optimizarlos continuamente. Esto también se apoya en el área de Gestión de la seguridad de la información a través del "Modelo de tres líneas de defensa".

- 1ra línea de defensa

  La primera línea de defensa está compuesta por la gestión operativa y es responsable de la definición, implementación y control de las medidas de seguridad de la información para el manejo de riesgos y el cumplimiento de los requisitos de seguridad de la información.

- 2da línea de defensa

  La segunda línea de defensa está en manos del CISO y la unidad de la seguridad de la información del Grupo ERGO, con el apoyo de las funciones de gestión de

riesgos establecidas localmente. La segunda línea de defensa define los requisitos de seguridad de la información y supervisa la definición, implementación y control de las medidas de seguridad de la información a través de la primera línea de defensa.

- 3ra línea de defensa

  La auditoría interna actúa como una unidad independiente como tercera línea de defensa y evalúa la efectividad de las primeras dos líneas de defensa.